WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

STATEMENT

on the notification of the German Draft Act on combating right-wing extremism and hate crime (2020/65/D)

Brussels, 22nd April 2020

On 17th February 2020, the Federal Republic of Germany submitted a draft act on combating right-wing extremism and hate crime to the European Commission for notification, filed under number 2020/65/D.

The German Federal Ministry of Justice and Consumer Protection (BMJV) presented a first draft of the act in December 2019. The draft is intended to strengthen the Network Enforcement Act (Netzwerkdurchsetzungsgesetz, NetzDG). Supplements to the German Telemedia Act (Telemediengesetz, TMG) and the German Criminal Code (Strafgesetzbuch, StGB) will oblige all providers and services which come under the remit of the TMG to collect and disclose user data and passwords. Finally, the existing powers of law enforcement and other security authorities are to be extended significantly.

In December 2019, eco – Association of the Internet Industry expressed considerable concerns about the first draft act. The changes in the act are expected to have serious consequences for telemedia service providers. At the same time, citizens may be confronted with encroachments on their right to self-determination – with regard to information in accordance with Article 2 (1) in conjunction with Article 1 of the German constitution (Grundgesetz) – as well as on their right to confidentiality, the integrity of information technology systems, and telecommunications secrecy. Accordingly, the national legislative process also has a bearing on the Charter of Fundamental Rights of the European Union (2012/C 326/02) and impinges considerably on this charter.

While prior to the submission for notification, the draft act was revised and concretized in some aspects, attention should be drawn to the following issues criticized by eco with regard to the notified draft act:

- Information obligations for telemedia service providers
- Obligation to disclose passwords
- Introduction of a reporting obligation in the NetzDG
- Country-of-origin principle not taken into account
- Overlooking of current legal developments at EU level

In summary, central points of the proposed legislation raise considerable questions concerning constitutional protection, fundamental rights, data protection, and the compatibility with European law, with these points requiring critical consideration.

Information obligations for telemedia service providers

With the draft act submitted for notification, the legislator has specified the requirements for the obligation to provide information on inventory and usage data for telemedia service providers. Section 15a TMG of the draft act creates a legal provision for the publication of data by providers of telemedia services.

The disclosure of inventory and usage data by providers of telemedia services is problematic in the context of constitutional and data protection regulations. The providers are obliged to release a considerable amount of personal data of conspicuous users and possibly uninvolved third parties, for example, data from dating portals or messenger services.

The new regulation allows for far-reaching encroachments to civil liberties, data protection, and telecommunications secrecy. The fact that the authorized bodies cited in Section 15a TMG are defined very broadly is problematic. In light of this provision, the obligation of telemedia providers to provide information extends to all authorities responsible for the prosecution of criminal, or even administrative, offenses, and for averting danger of public safety. These include, for example, all of the federal and state secret services, the customs administration, and offices which are responsible for, among other things, combating illegal employment.

Inventory and usage data may also be expressly released if the data is used to prosecute simple crimes and administrative offenses. Taking all circumstances into account, the proportionality appears questionable. As a result, it becomes clear that the legislator has underestimated both the qualitative and the quantitative dimensions of the new provision in the German Telemedia Act and has not sufficiently considered the impact and consequences for telemedia services.

The proposed regulation affects not only the operators of social networks but all services which fall under the German Telemedia Act and thus all telemedia services provided on a commercial basis: be it email, website or forum, online shopping, chat and messenger, or cloud services.

Obligation to disclose passwords

The submitted draft act also provides for an obligation by telemedia service providers to disclose passwords, based on Section 15b TMG. While the legislator has clarified that the issuing of passwords is linked to a judge’s reservation and is permissible for the prosecution of particularly serious criminal offenses, the issuing of passwords is still to be evaluated critically.

In the latest update, the legislator clarified that there is no obligation to safeguard unencrypted passwords. Such an obligation would have led to a huge setback regarding cybersecurity and data protection. However, with a successfully decrypted password, the requesting authority would not only be able to access or extract information from the user, but also to take over the user’s account, or rather the digital identity and, among other things, to also act on behalf of the account owner vis-á-vis third parties.

Such a far-reaching authorization to disclose passwords will influence the users’ trust in digital services. For providers of telemedia services, the disclosure of passwords is also considered questionable, because a password may also enable access to third-party services, linking storage space and terminal equipment.

Introduction of a reporting obligation in the NetzDG

The existing provisions of the NetzDG are to be supplemented by a reporting obligation introduced with the amendment. On its basis, operators of social networks are obliged to report flagged content which has been deleted or blocked

for being illegal to the Federal Criminal Police Office (BKA). In addition to general information on the publishing user and the corresponding content, the report to the BKA shall include the IP address and the port number of the publishing user, provided that this is available to the operator of the social network.

On the basis of this obligation, sovereign tasks in the digital context will be transferred to private companies. With the obligation to collect, store, and report IP addresses and port numbers, social network operators will be obliged to process sensitive user data and transmit it to the BKA without any concrete evidence of a criminal offense.

The legal justification for operators to report allegedly illegal content does not exist. For the identification of the purportedly illegal content, a proper legal assessment of each individual case will be necessary. A legal assessment, however, is not possible due to the short processing times of the NetzDG. Instead, operators of social networks will have to proactively forward content and user data to the BKA on the basis of a possible suspicion. This proactive release of user data contravenes Article 15 (2) of the E-Commerce Directive (2000/31/EC).

As a consequence of the reporting, within a short period of time, an extensive database consisting of social network users suspected of infringing the law, content, and other information will be created at the BKA on the basis of the submitted reports. Despite critical comments by eco, the legislator has still not created a clear legal basis for the collection, processing, and deletion of the data accumulated by the BKA. On the other hand, private companies are bound by a fixed set of rules for handling personal data, for example by the European General Data Protection Regulation. They will be placed in a conundrum where they have to guarantee that collection, storage, and transfer of personal data takes place in compliance with the framework of the GDPR and under the risk of its high financial penalties.

Overall, it remains highly uncertain as to whether a reporting obligation is sufficient to combat right-wing extremism and hate content on the internet. The experience of the eco Complaints Office shows that a consistent and effective response to these problems requires the inclusion of the jurisdiction and law enforcement agencies. Therefore, it is essential that the technical and human capacity, as well as the competencies of criminal follow-up and investigation bodies, be strengthened. This is a preferable and more efficient option.

Country-of-origin principle not taken into account

Doubts regarding the conflict of the NetzDG with European law have already been raised during its legislative procedure and have not yet been dispelled. In the future, providers of telemedia services, independent of their place of business, will be required to comply with investigation and reporting obligations under German law.

Such obligations conflict with the country-of-origin principle in the E-Commerce Directive (Art. 3 and Rec. 22):

‘Information society services should be supervised at the source of the activity, in order to ensure an effective protection of public interest objectives;’ and, ‘it is essential to state clearly this responsibility on the part of the Member State where

the services originate; moreover, in order to effectively guarantee freedom to provide services and legal certainty for suppliers and recipients of services, such information society services should in principle be subject to the law of the Member State in which the service provider is established.'

If the German example sets a precedent this could, in consequence, lead to a fragmentation of the Single Market.

Current legal developments at EU level

With the notified draft act, the Federal Republic of Germany is attempting a further regulatory solo effort in Europe. Examples of similar efforts relate to the proposed E-Evidence Regulation, the Terrorist Content Online Regulation, the announced Digital Services Act, and the Code of Conduct on countering illegal hate speech.

Even before the notification of the current German Draft Act to the EU Commission, the latter commented on the notification of the French legislative procedure for combating hate content on the Internet. In its response, the Commission stressed that it is seeking a uniform legal approach within the EU framework of the Digital Services Act. Ultimately, the Commission was asking the French Republic to suspend the national legislative procedure (C(2019) 8585 final of 22nd November 2019).

Accordingly, the fact that the Federal Republic of Germany is once again pushing ahead in the European context with the draft act submitted for notification must be censured. Just why it has submitted two drafts for the extension and revision of the NetzDG within a short period of time, instead of becoming involved in the European legislative process, remains unclear.

Conclusions

eco is fully committed to the fight against right-wing extremism and hate crime and supports the fight against illegal content online.

The concerns of telemedia service providers regarding the high degree of intervention possibilities in the issuing of passwords have not been eliminated by splitting the provision into Sections 15a and 15b TMG. The clarifications made still leave questions unresolved and leave the companies with legal uncertainties.

At the point of the introduction of the NetzDG, the legislator had already promised that an evaluation of the act and its effects would be conducted. The fact that two legislative procedures for the expansion and amendment of the NetzDG are being presented simultaneously (the Act to Combat Right-Wing Extremism and Hate Crime and the Act to Amend the NetzDG) is questionable, especially given that no results from the evaluation of the act are yet available. Instead of transferring further obligations to social network operators with each reform, the legislator must ensure that the criminal investigation and prosecution authorities are in the position, both technically and from a personnel perspective, to combat hate and incitement to hatred on the Internet.

The notified draft act takes neither the country-of-origin principle under Art. 3 nor the requirements for reactive disclosure of data with Art. 15 of the E-Commerce Directive into account. The provision of user information and content to responsible authorities is in breach of the General Data Protection Regulation and Directive

(EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by the responsible authorities for the purpose of the prevention, investigation, detection, or prosecution of criminal offenses or the execution of sentences. With the notified Draft Act, user rights will be circumscribed or removed, and providers of telemedia services will be obliged to disregard existing EU legislation.

Furthermore, the national legislative process also has a bearing on the Charter of Fundamental Rights of the European Union (2012/C 326/02) and impinges considerably on this Charter. Already with the implementation of the NetzDG and its obligations, a restriction of freedom of opinion und information under Article 11 of the Charter was expected. The German legislator wanted to examine the concerns and effects with an evaluation of the NetzDG. However, the results of the evaluation are still not available. The additional obligations of the notified Draft Act will violate further fundamental rights, in particular the respect for private and family life under Article 7 of the Charter, the protection of personal data under Article 8, and the freedom to conduct a business under Article 16.

About eco

eco – Association of the Internet Industry e. V. is an advocate for and promoter of all companies that create economic value with or on the Internet. The association represents more than 1,100 member companies. These include ISPs (Internet Service Providers), carriers, hardware and software suppliers, content and service providers, and communication companies. eco is the largest national Internet Service Provider association in Europe.